USAWC STRATEGY RESEARCH PROJECT

AN EMERGING STRATEGIC CONCEPT – EFFECTIVE INFORMATION OPERATIONS (IO)

by

Lieutenant Colonel Jess A. Scarbrough
US Army

Mr. Frank Jones
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Jess A. Scarbrough (LTC), USA

TITLE: An Emerging Strategic Concept – Effective Information Operations (IO)

FORMAT: Strategy Research Project

DATE: 07 April 2003 PAGES: 30 CLASSIFICATION: Unclassified

The 2001 Quadrennial Defense Review (QDR) Report describes six critical operational goals for transforming the Department of Defense to include DOD/JCS headquarters staffs and the military departments. One goal in particular clearly asserts that we must assure our information systems can survive in the face of an attack; and we must likewise conduct effective offensive information operations (IO). This strategic research paper assesses information operations within the Department of Defense and the services, will propose a conceptual information operations force structure model as a basis to frame force structure decisions, provide a force structure effectiveness rating based on historical examples and will conclude by recommending and implementing a Defense Information Operations Agency (DIOA). DIOA will be designed to provide a synergistic effect with regards to IO and to the stated IO objectives highlighted in the 2001 QDR report.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

AN EMERGING STRATEGIC CONCEPT – EFFECTIVE INFORMATION OPERATIONS (IO)

Information Operations (IO) involves actions taken to affect adversary information and information systems while defending one's own information and information systems.[1] This emerging concept is essential for the Joint Force Commander to achieve his objectives as dictated by our Commander-in-Chief, the President of the United States. Technological advances over this past decade in the area of informational systems have been tremendous. These advances, plus the dedicated resources that we have placed in the development of military informational systems, has allowed the United States to project our national interests worldwide more rapidly then ever before. However, as these advances become more known to the international community, we must understand that some of the world's international actors will want to counter them and could be a threat to us. Therefore, we must be able to identify threats, and use a synchronized information operations campaign that brings the full force of our capabilities to generate the necessary effects to protect and defend the United States.

This strategic research paper will assess the elements that form the basic doctrine of information operations as defined by the Office of the Secretary of Defense (OSD) and the Military Departments, to include the service core competencies. From this information, conclusions that the government should tie all the service information operations programs into a single coordinated agency. The principal reason for this approach is twofold: (1), to generate a coordinated information operations effect that the Joint Force Commander can use and employ as an information superiority enabler, and (2), to draw on limited resources to maximize our investment to the fullest possible extent. Further, this paper will propose a conceptual model for framing information operations force structure decisions and using historical cases, devise a force structure effectiveness rating. This paper will conclude with a recommended Defense-wide organization that will bring into focus full spectrum IO and incorporate all the established elements of IO that support the transformational goals in the United States Defense Department's 2001 Quadrennial Defense Review report. This organization will be able to take full advantage of our technological advances in order to keep the United States military the preeminent military force in the world and protecting our national security.

OSD AND SERVICE IO PERSPECTIVES

The 2001 Quadrennial Defense Review (QDR) Report described six critical operational goals that provide the focus for the Department of Defense's transformational efforts. One goal in particular clearly asserts that the Department of Defense must assure our information

systems can survive in the face of an attack and that the Department must be able to conduct effective offensive information operations.

Information and space operations are new dimensions of conflict. They require a backbone of networked, highly distributed capabilities. The 2001 QDR states that defense planning must recognize these new requirements and address vulnerabilities in both Information and Space doctrine".[2] The Assistant Secretary of Defense (C3I) further prescribes there are several elements within full spectrum information operations that defense planners must consider. These elements include psychological operations, military deception, electronic warfare, physical destruction, sensitive information operations, information assurance, physical security, operational security, counter-psychological operations, counter-intelligence, computer network attack, and command and control protect.[3] Department of Defense information operations doctrine calls for force structure decision makers to account for all these elements in order to draw upon these capabilities and make effective use of information operations, which can shape the strategic and operational environments. OSD has emphasized that the employment of information operations assets needs strong interagency coordination, clear targets, synchronized activities, and the support of timely intelligence, which has to be integrated into the planning process. If information operations assets are properly employed in a coherent manner, then the intended effects have a high probability of succeeding within the full spectrum of military operations including MOOTW. Furthermore, information operation planning must be accomplished in both the deliberate and crisis action planning processes and be incorporated in the Joint Force Commander's overall operations planning.[4] Lastly, information operations planning must be broad based and encompass all activities in the planning process – Joint, Service, Interagency, and Multinational.

The Departments of the Army, Air Force, and Navy have developed techniques for information operations employment unique to their respective services. A brief discussion is required to further understand how the services have formulated IO doctrine based on their core competencies.

Army Field Manual 100-6 addresses Army information operations. According to the manual, US Army information operation efforts must center on all the phases of military campaign planning. Army defines information operations as an information dominance enabler. Information dominance is defined as the degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary.[5] A key step toward achieving information dominance is when the commander's

level of battlefield visualization and situational awareness is achieved and the enemy's grasp of situation is significantly degraded. The key information operations objective for Army commanders is to influence, disrupt, or delay the adversary's military decision-making cycle while protecting United States and/or coalition decision-making cycles.[6]

The Army stresses three areas of information operations. These areas incorporate, to some extent, the elements of IO that OSD has highlighted within its policy guidance. Command and Control Warfare (C2W), Civil Affairs Operations (CA), and Public Affairs Operations (PA) are the three fundamental cornerstones of Army Information Operations doctrine.[7] C2W includes operational security, military deception, psychological operations, electronic warfare, and physical destruction. CA activities encompass the relationship among military forces, civil authorities, and people in a foreign country or area. PA fulfills the commander's obligation to keep the American people and the soldiers informed.[8] Commanders employ these elements of information operations in order to gain an operational advantage on the battlefield.

The Air Force states their key objective in information operations is to gain information superiority, which leads to aerospace supremacy. Aerospace supremacy is focused at the strategic level and information superiority leads to the domination of the skies. The Air Force believes that dominating the information spectrum is as critical to winning today's conflict as controlling air and space or occupying land was in the past and is seen as an indispensable and synergistic component of aerospace power.[9] For the Air Force, information operations comprise those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare and are conducted throughout all phases of an operation and across the range of military operations.[10]

Information-in-Warfare (IIW) involves the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities.[11] Information warfare (IW) is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems.[12] Two key elements that drive Air Force information warfare doctrine are offensive counter-information (OCI) and defensive counter-information (DCI).[13] Within these elements the Air Force employs a range of full spectrum information operations techniques, such as, electronic warfare, deception, computer network attack, computer network defense, information assurance, and public affairs, to support the Joint Forces Commander within the Joint Forces Air Component Command.

The Navy's main goal in information operations is to support their maritime dominance of the high seas. According to naval doctrine, the Navy must be positioned to take advantage of the opportunities offered by Information operations, and it must be alert to the imperatives that information operations impose on the success of sea power undertakings.[14] The Navy should seek methods in the area of information operations to deter, degrade and influence potential adversary's information systems. Applicable IO elements include both offensive and defensive IO, are operational security, computer network attack, electronic warfare, physical destruction, deception, psychological operations and public affairs.[15]

In reviewing service IO perspectives, one can draw two obvious conclusions. One, each service is using the technique of information operations as an information dominance enabler to gain a significant tactical or operational advantage. Two, each service has drawn on methods or elements of information operations in order to enable or advance their core competency within the national military instrument of power but their objectives are not necessarily in consonance. One can argue that their approaches actually hinder the most effective use of the military instrument. Therefore, in a resource constrained environment, the Department of Defense must develop a central agency of information operations elements in order to harmonize requirements, to meet the stated QDR 2001 transformational goal, and to get the best possible equipment to maximize our information operations capabilities.

PUTTING IO DOCTRINE INTO PRACTICE

Major General Carl Von Clausewitz wrote "war is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means."[16] If war is truly instrument of policy by other means, then all decisions made in the preparation of war are a matter of policy and not procedure. This reality underscores the critical importance of peacetime planning. One of the most critical planning elements is force structure. Poor force structure decisions can lead to mission failure and loss of life – problems that cannot be resolved by commanders under fire.

Force structure decisions are generally made for the good of the nation. Within democracies, soldiers' interests are also considered. These decisions must be somewhat tentative in view of global dynamics; however a maturing society is always searching for better ways to serve its people and to further its interests. In *The Prince*, Machiavelli suggested "Whoever desires constant success must change his conduct with the times."[17] The nature and scope of complex force structure decisions provide grounds for intellectual battles, while the nation hopes that our leaders have made the correct decisions. That is where this paper joins

the debate by presenting an alternative view of future force structure decision-making that ensures the synergy of information operations tools so as to provide our national leaders with the fullest range of information operations options.

New missions and new realities require new systems, procedures and operational concepts. However, all of these must fit into a strategic force structure model that meets the threat and can be expected to help commanders to perform its missions. The proposed information operations force structure model (IOFSM) consists of three critical components.[18] Each of these components supports the Department of Defense's Quadrennial Defense Review 2001 Report's critical operational goal of information assurance and information operations. This model addresses the growing importance of information in operations and warfare.

Active information operations are based on protecting the execution of the United States national security strategy according to the 2001 QDR. The model takes into account all the national instruments of power, to include national political, economic, and military strategies. The proposal recommends three modes within the information operations force structure model (IOFSM) that would span the full spectrum of conflict that the United States is faced with in today's environment. These modes are pure information operating systems or forces (PIOSF) dealing with one extreme and pure physical destruction (kinetic) systems or forces (PPDSF) dealing with the other extreme. In the center of these two extremes, would be combined operations that would include a mixture of pure information operating systems or forces (PIOSF) and pure physical destruction systems or forces (PPDSF). Figure 1, displayed below, graphically portrays these modes.

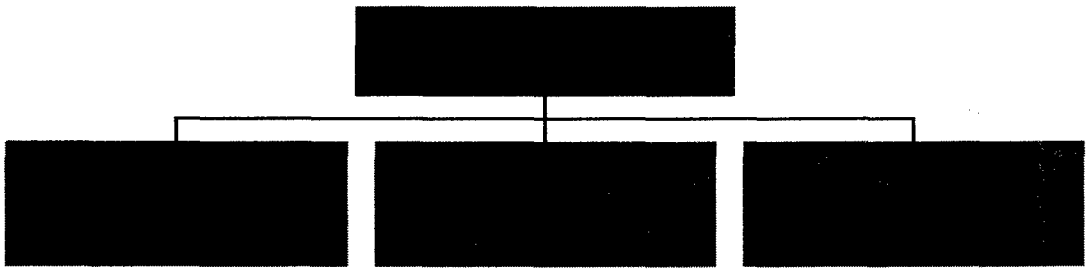

FIGURE 1. INFORMATION OPERATIONS FORCE STRUCTURE MODEL

Pure physical destruction systems or forces (PPDSF) can be termed as pure kinetic warfare. PPDSF are engaged in operations relying on the exclusive use of physical force without the benefit of information. These operations are conducted by warriors employing weapons of physical destruction in the extreme without knowing fully who, what and why. An example is a fielded army in the heat of battle where the original operations plan is no longer

applicable and the troops react to their situation with total destruction in order to survive. Though this type of operation is becoming rare because it represents the ultimate expression of pure violence, we must keep in mind that war, once unleashed, can develop ends of its own, making it difficult to control. Therefore, the unrestricted use of violence is always a possibility.[19]

The existence of pure physical destruction systems or forces (PPDSF) that are so totally devoid of information that it is difficult for us to imagine this mode would be used today. Past military leaders and theorists could understand this approach because war was the ultimate expression of physical destruction and the tools they needed to accomplish their political objectives did not depend on information operations/systems. Generals used their soldiers to battle and threw them into the breech as best they knew how in order to achieve victory at the decisive point of attack. As the battle unfolded, it inevitably came to a point where the effective application of violence, sheer strength in numbers, and the will of the army combined to determine the outcome of the battle.[20]

Today we do not have many examples of this type of operation. One step above PPDSF is the directed, yet indiscriminate, immoral bombing or shelling of targets. Although these operations support a larger effort, the indiscriminate character marks them as a purely kinetic operation. However, today military forces employing physical destruction capabilities are nearly always combined with significant information forces, categorizing these operations in the center mode of operations employing a mixture of PPDSF/PIOSF.

The employment of modern day forces are typically under the command of a joint forces commander, who uses sophisticated command and control forces. These forces collect, process and disseminate information that can be used to employ purely kinetic weapons to destroy their targets and break the will of their enemies. As the United States continues to modernize our military force, a key factor in using this mode will be to understand thoroughly the relationship between informational type forces and forces of physical destruction.[21]

Joint Vision 2020 outlines the ultimate use of combined PPDSF/PIOSF as it expands on the concept of "information operations" throughout the full spectrum of conflict during peace and war.[22] Force structure planners need to determine the right mix of informational forces and kinetic forces when validating the requirements. The reason for this is to utilize the full capability of our technologies. These forces must be integrated into a coherent joint operational concept. This issue will be discussed later in terms of a single information operations organization.

Today, the overwhelming majority of day-to-day operations can be classified in our last mode – pure information operations systems or forces (PIOSF). During peace (peace

enforcement operations, peacekeeping operations, etc.), PIOSF in the strictest sense is our most dominant form of information operations. Technology has enabled the military to gather increasing amounts of information, process that data, and provide a reasonably coherent assessment of the situation to our national leaders. They, in turn, can use the government's national instruments of power – political , economic, military and/or informational – to accomplish our national security objectives.

Now that we have discussed in some detail the three modes of our information operations force structure model, the right mix of forces must be determined in order to gain the ideal force structure effectiveness rating.[23] On one end of the spectrum, we are assessing the percentage of the total force engaging in kinetic systems or forces and on the other end we are assessing the percentage of the total force engaged in pure informational systems or operating forces. As the spectrum of conflict changes, force structure planners want to ensure that there are effective forces in place to accomplish all assigned missions within an assigned area of responsibility. Ideally, for every international situation we are faced with - war, low intensity conflict, or humanitarian operation – there is an optimal point where the appropriate amount of kinetic systems or forces are matched to the appropriate amount of informational systems or forces.

The concept displayed in Figure 2 forms a basis upon which one can connect force structure decisions to the appropriate mix of the proposed modes of the IOFSM – pure physical destruction systems or forces (kinetic force element), pure informational operation systems of forces (informational force elements), or combined PPDSF and PIOSF – spanning the full spectrum of peace and war (as depicted as the increase in the level of violence). By showing force structure effectiveness as a function of kinetic and informational force structure elements, this graph provides a readily comprehensible means of securing the ideal force construct – a quantifiable basis to validate an acquisition requirement. In addition, Figure 2 forms the foundation for the eventual development and procurement of information operating systems based on the three modes of our proposed IOFSM.

Figure 2 depicts two opposing symmetric slopes. The solid slope represents kinetic force elements which are defined as the coercive elements of force which compel an adversary to do our will through physical force or as an effective flexible deterrent option (FDO). Basically, these are the forces that are physically capable of killing people and destroying the enemies weapon and C2 systems by means of kinetic energy. The dashed slope represents informational force elements. These forces include the nation's entire information infrastructure, both military and civilian. Essentially, the informational force elements include all public affairs

agencies, and command and control forces responsive to, or capable of being commanded by, the United States Government as part of either crisis or deliberate action planning.

The intersection of the slopes indicates the point of ideal force structure effectiveness. For every situation faced in the international arena – every crises, conflict, war, humanitarian operation, peacekeeping operation, peace enforcement operation, etc. – there is an ideal point where the appropriate mix of informational force elements matched with the kinetic force elements creates an ideal force structure. The objective of any force structure planning process is to identify the ideal force structure mix. In terms of historical application, creating the ideal force structure mix can be equated to applying the appropriate amount of force against the right targets at the correct time.

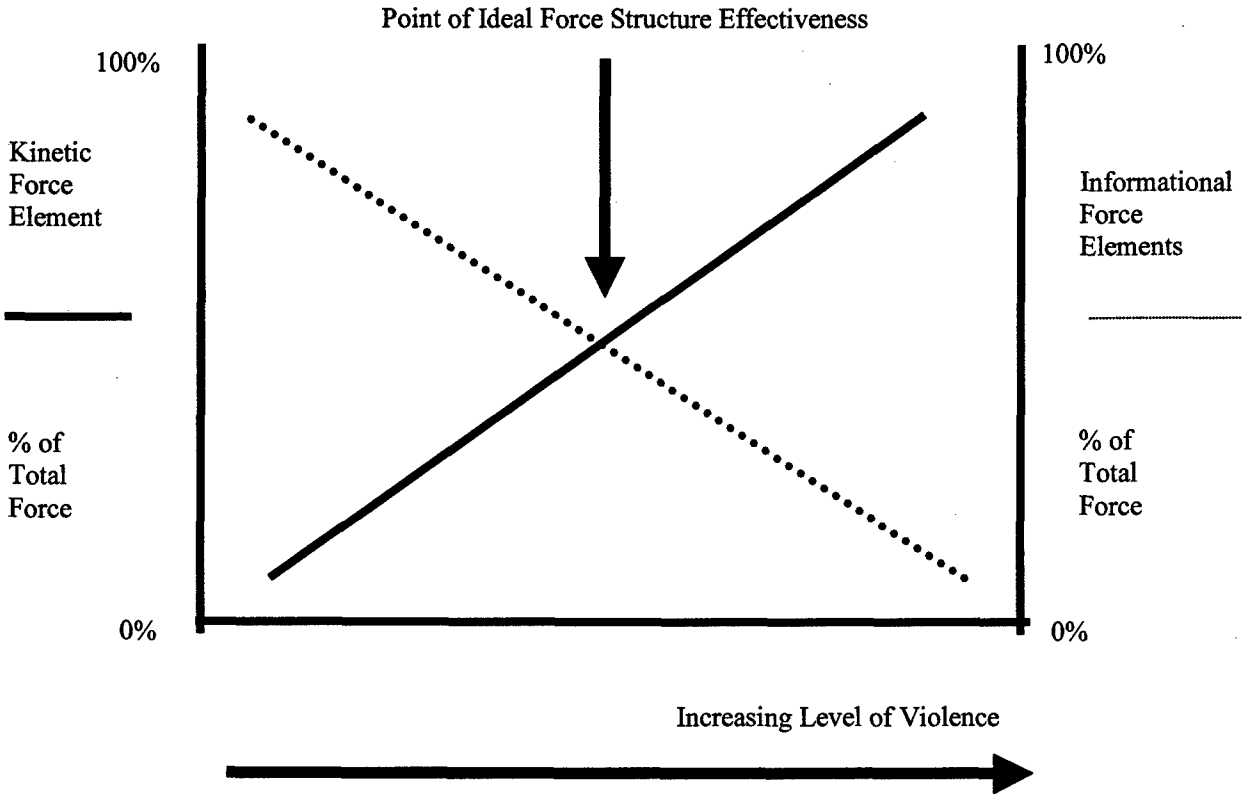

FIGURE 2. FORCE STRUCTURE EFFECTIVENESS GRAPH

By using the above force structure effectiveness graphical representation and applying the three modes of our information operations force structure model (IOFSM), one could apply a rating (a force structure effectiveness rating – FSE) using some recent historical examples of military application and force structure decisions. Such examples could include, the bombing incident of a incorrectly identified target that later was found out to be a passenger train carrying

civilians over a bridge in Serbia, the prosecution of Operation Desert Storm, and the development of our Strategic Nuclear Forces/Operations during the Cold War.

The civilian bombing incident in Serbia represents a situation where inaccurate information was assessed. For the purposes of this model, inaccurate information equates to no information. Graphing our appropriate points on the slopes of our chart (see Figure 3), actual events permit us to place our first point low on the informational slope (point A).[24] Since this information was not complete and did not accurately describe the threat, a point low on the informational plot represents the lack of value that the information contained. Logic would follow, that a force structure package that did not provide accurate information and a force structure package that utilizes a very high percentage of kinetic elements, could be risky for achieving the desired outcome based on mission objectives. Therefore, a plot would be placed at a point high on the kinetic force element slope (point B). On our scale, the product of the two plots results in a very low FSE rating. Therefore, the ideal force structure mix was employed and the result was a public affairs debacle for the United States.

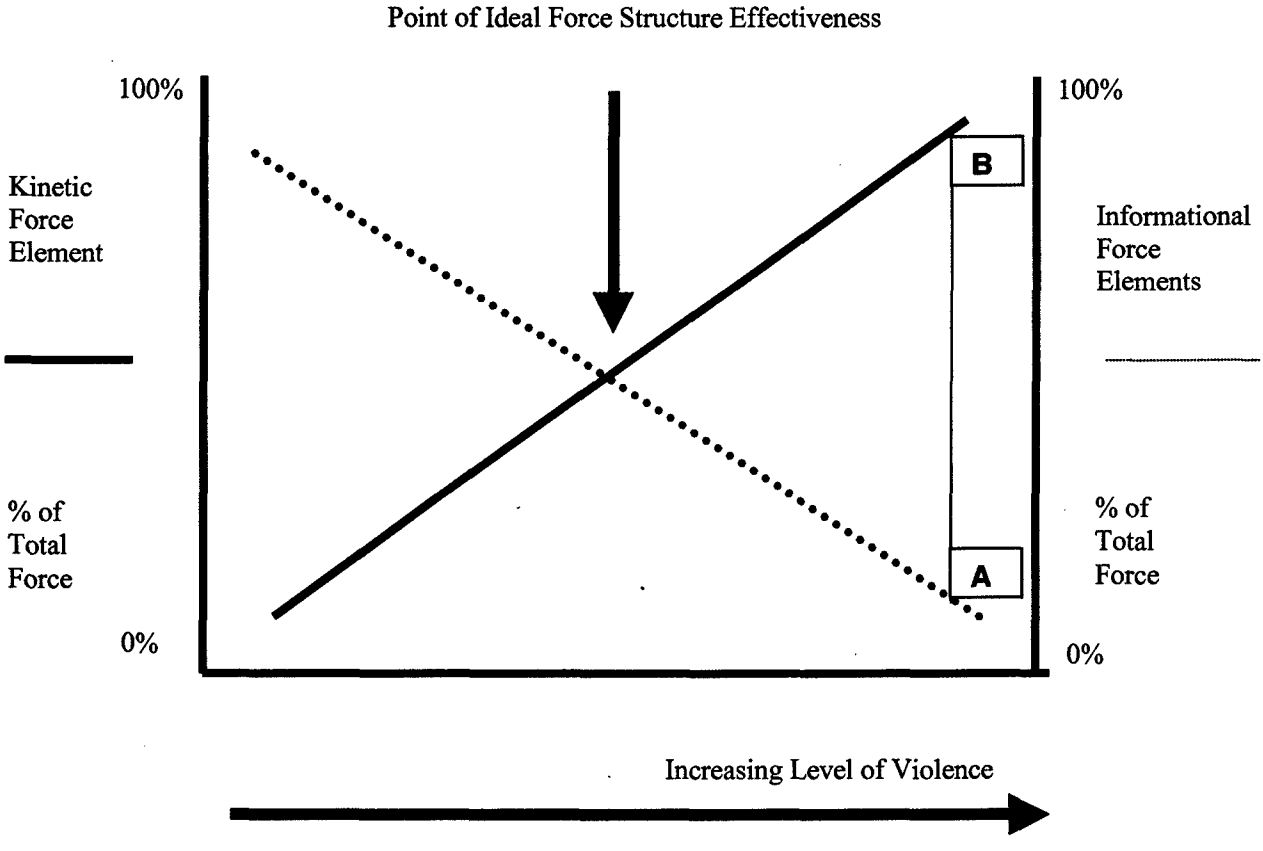

FIGURE 3. FORCE STRUCTURE EFFECTIVENESS GRAPH CIVILIAN BOMBING INCIDENT

Desert Storm (Figure 4) offers another example of exposing both the strengths and weakness of the proposed information operations force structure model.[25] We used significant amounts of information to apply kinetic forces in overwhelming numbers in a way the world has never seen. The United States and her allies utilized flexibility, synchronization, speed, and precision that are unmatched in history of military art.

Making use of the FSE graphical representation (see Figure 4), the United States should feel completely justified in plotting a point high on the kinetic force element slope (point B), acknowledging the overwhelming role of purely physical destructive systems or forces in the war. According to the US Government Accounting Office, "92 percent of the total bomb tonnage dropped was dropped in the form of unguided dumb bombs." More telling is that, "95 percent of the total bombs dropped against strategic targets were unguided as well".[26] While dumb bombs were dropped costing millions and millions of dollars and dropping thousands of tons of ordinance on armored vehicles in the open desert, it did not result in the efficient use of our informational forces. This type of warfare is better described as PPDSF and clearly represents the majority of operations in Desert Storm. Correspondingly, our plot on the informational element slope would be low acknowledging the limited focus of PIOSF in the war (point A).

The product of this rating (low FSE rating) does not, at first, equate with the results of the war. However, when considering how much more effectively the war could have been waged had the ratio between the informational forces and the kinetic forces been more appropriately matched, we can begin to accept this low rating. Informational forces were utilized in the Gulf War and they played a larger role than in past wars, but the war was unequivocally fought with purely physical destruction systems or forces.[27] Therefore, the ideal force structure effectiveness rating was not achieved, even though the results of the war addresses clearly of the modern firepower the United States military possesses and its successful use.

For the force of the future to be effective, it must have an accurate mix of mutually supporting kinetic and informational forces. Adhering to the practice of overwhelming force drives decision makers to provide abundant resources which in turn can lead to the procurement and deployment of purely kinetic forces. These kinetic force expenditures are at the expense of the informational forces. As a more practical matter, the finite resources available are too limited to squander in implementing inefficient attrition warfare techniques. Resolution of this extremely complex issue will only begin when the senior DOD leadership begins to promote thorough analysis of emerging information doctrines and structures. In this way, we can begin to identify effective information and kinetic force structure ratios appropriate

to our future needs and begin to move away from our continued reliance on industrial age, attrition warfare paradigms.

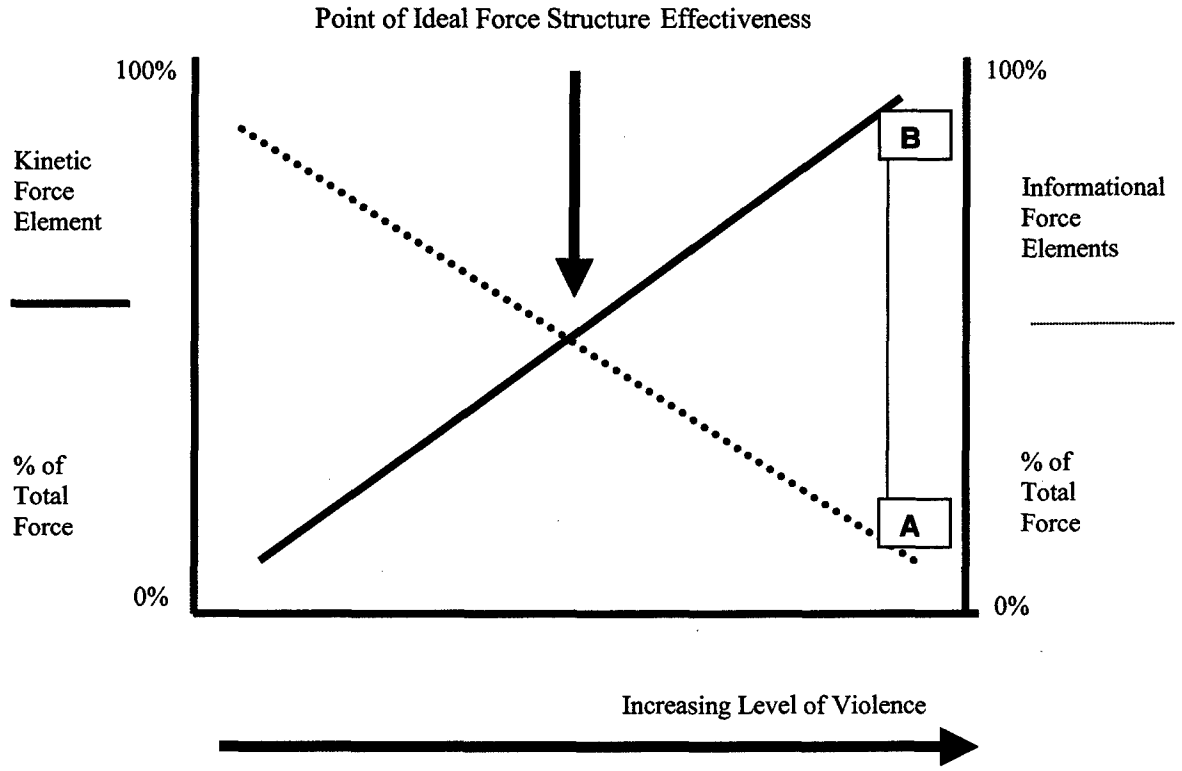

FIGURE 4. FORCE STRUCTURE EFFECTIVENESS GRAPH DESERT STROM

However, there is one mission area where the force structure effectiveness rating was successful and lessons learned can be concluded. This was the mission area of strategic nuclear operations (Figure 5).[28] Since information was so critical in the employment of such devastating weapons, the force structure mix had to be correct. The result of an error in this mission area would have been disastrous for not only the United States but for the entire world.

The mission to deploy nuclear forces and conduct actual exercises was extremely successful for over fifty years. This mission was the linchpin of the United States' strategy of containment. On the force structure graphical representation (see Figure 5), data indicate plots would be annotated high on both the informational force element slope (point A) and the kinetic force element slope (point B), resulting in a high FSE rating. Nuclear forces had to maintain a focused command and control infrastructure that relied on tailored informational forces to be effective. If force had to be used, informational forces would directly control a measured nuclear

response, that is, employment of the United States' physical destructive systems or forces. Therefore, the force structure effectiveness had to be high because any miscalculation would have been possibly our last.

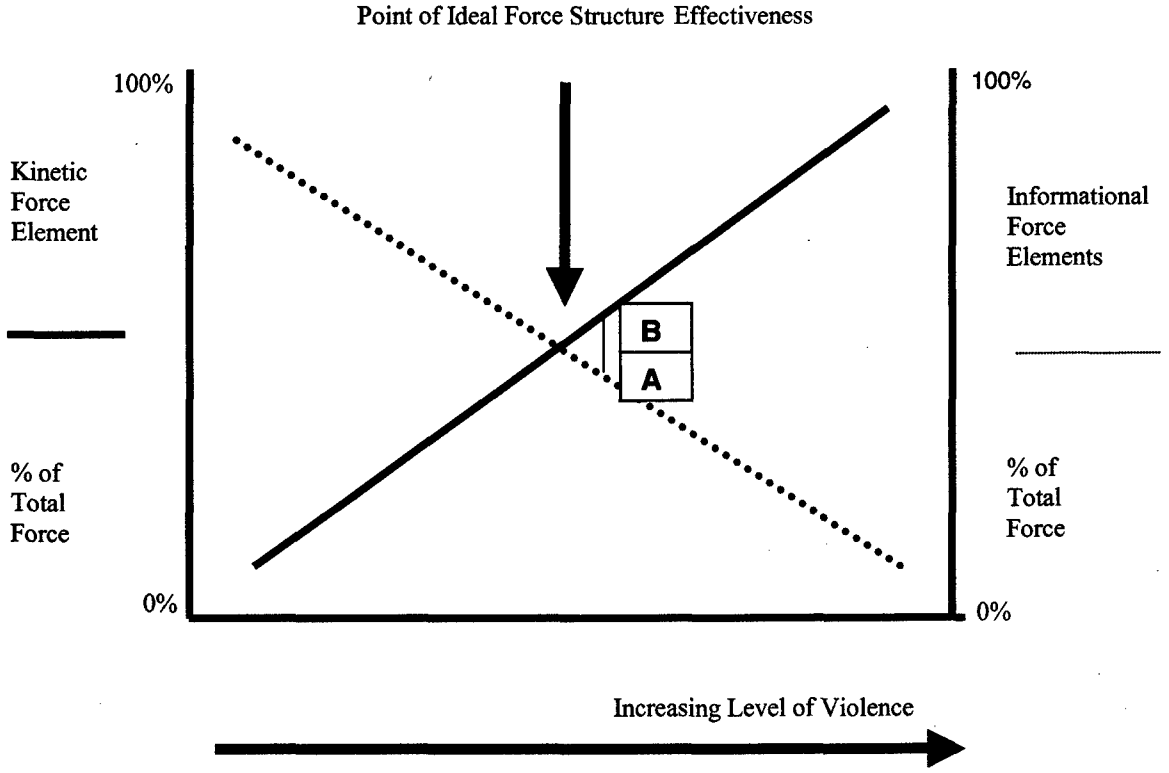

FIGURE 5. FORCE STRUCTURE EFFECTIVENESS GRAPH STRATEGIC NUCLEAR OPERATIONS

RECOMMENDED INFORMATION OPERATIONS AGENCY

Based on the analysis in the Department of Defense (DOD) 2001 Quadrennial Defense Review; the DOD and military departments doctrine on undertaking information operations; the three modes within the proposed information operations force structure model (IOFSM) framework and the derived force structure effectiveness rating, we are now ready to recommend a possible organization. This organization should be able to reap all the focused capabilities of using informational forces in order to minimize, initially, the use of purely physical destructive systems or forces, or, if needed, to use overwhelming force at the right place and the right time to achieve a quick result, thereby stabilizing a situation as soon as possible.

An effective IOFSM concept has the potential to greatly increase the efficiency of the currently disjointed and disparate information operations conducted in military departments by breaking down the "stovepipes" and effectively flattening the information operations structure. The IOFSM provides a framework to meet the future needs of the nation in the information age.

The conceptual basis for a Defense Information Operations Agency (DIOA) is based on the three modes discussed earlier within the IOFSM. At the top of such an organization is the single authority responsible directly to the President of the United States and the Secretary of Defense. This individual would direct three principal sub-organizations (see Figure 6) responsible for recommending IO based solutions to any situation within the full spectrum of conflict.

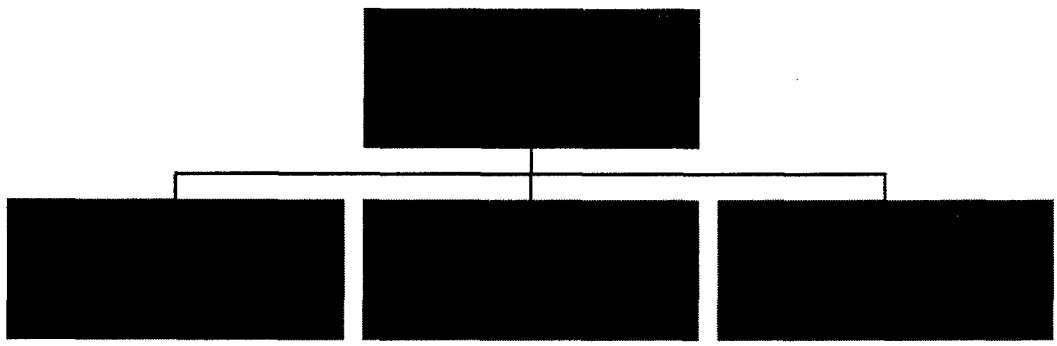

FIGURE 6. PROPOSED DEFENSE INFORMATION OPERATIONS AGENCY

One of the sub-organizations would be founded on the principle of employing pure informational operating systems or forces (PIOSF). Within this element, a break down of information operations assets into offensive PIOSF and defensive PIOSF would be proposed. These forces would be organized to support the President's national instruments of power: political, economic, information and military. The elements of full spectrum information operations would be utilized to gain the appropriate effect.

The information operations assets within the offensive PIOSF sub-organization could or would be used to compel an enemy to conform to our national objectives. Psychological operations would be employed to gain operational objectives that support the political, diplomatic and economic instruments of national power. Psychological operations would be beneficial as well to control certain critical infrastructures (telecommunication systems) that can offer assistance to their own people after a situation has stabilized in a certain country or region. Another example of the PIOSF offensive approach is the use of electronic warfare, military deception, and exercises influence to effect the President's military instrument of national

power. As an example, these elements of information warfare would be specifically used to manipulate a country's political control and data acquisition systems, computer operations, and communications systems.

Defensive PIOSF would embrace the information operations elements of command and control protection, information assurance, operational security, communications security, and counter psychological operations. These elements are valuable to counter hostile information operations used only by pure informational operational forces. Command and control protection is actions taken to secure computer network operation, secure communications and counter any adversarial psychological or proganda information designed to hurt the national security of the United States.

Pure information operations systems or forces (PIOSF) must always be the first option to employ in order to gain the proper force structure effectiveness rating. As you employ your informational forces, and if conflict cannot be avoided, then a good by-product (this could be termed second, third or fourth order of effect) of this initial effort is that sufficient information has been acquired to effectively use a combined PIOSF and PPDSF or pure kinetic forces. The idea is to use the pure informational operating systems or forces as much as you can to possibly preclude use of pure physical destruction, or, at least, to minimize potential destruction.

Combined pure information operations systems or forces and pure physical destruction systems or forces would be the next sub-organization within the Defense Information Operations Agency. Again, this sub-organization would be organized into offensive and defensive elements. Offensive PIOSF/PPDSF would be used to influence an information operations attack as envisioned in the Joint Vision 2020. Defensive PIOSF/PPDSF would be used to counter any potential adversaries information operations initiatives. These employment techniques could be categorized into the mission areas of counter-kinetic, counter-C4, counter-ISR, and counter-EW.

The key focus within the combined information operations and pure physical destruction forces would be to search and find the appropriate force structure mix to accomplish the specific objective or objectives as outlined by our national strategic leaders. This sub-organization would always need to reassess situations in order to recommend the optimal forces to achieve the appropriate effects, which in the future will predominately be non-physical in nature rather than kinetic.

The last sub-organization within our proposed DIOA would be a staff element to focus on the possible use of pure physical destruction systems or forces. This element would always interact with the other sub-organizations in order to collect and assess critical and accurate

information. If a pure kinetic solution is in order, accurate information will be needed to recommend the most appropriately tailored force. This is absolutely critical because the idea is to use force overwhelmingly and quickly in order to regain stability rapidly. This would allow the other sub organizations to use their informational operating forces to gain the appropriate effect by fully leveraging the President's national instruments of power.

Based on this conceptual DIOA organizational concept, we turn our attention in creating such an organization. A three-pronged approach is recommended in implementing such a task. First, we must first organize to modernize the force. Secondly, we must improve the required analytical foundation to achieve the ultimate objective of enabling the application and expansion of the requirements process across the entire DOD. Finally, change has to be conveyed as the overwhelmingly right thing to do in order to prevent people from not buying into new requirements that prevent the completion of the first two prongs.

As we organize to modernize our informational forces, we need to establish and describe clear lines of authority and the proper organizational structure. The lines of authority and organizational structure need to parallel the three sub organizational elements in order to take advantage of all of the country's valuable information resources. We need to develop coherent arguments that express the benefits of this proposed organization in order to convince the United States Congress to amend Title 10, USC. This amendment is needed to support fiscally such a massive change within the Department of Defense. The first step that must be taken is to create a furor and excitement for such a change that convinces the Congress and the public that an active information operations campaign would enhance the security of the country. The second step is to develop a coherent requirement in size and scope that allows service departments to tailor a force based on the informational data to meet a national objective against a particular situation.

To overcome the obstacles of the second step, we must improve our analytical capabilities so that force structure planners can render better judgments when determining the trade-offs of a kinetic system over a information system, or, vice versa. The need for a common baseline of comparison is a prerequisite for the proper functioning of the current force structure requirements process and thus, cannot be overlooked or ignored despite the challenges.

At the apex of the Department of Defense requirements process is the Joint Requirements Oversight Council (JROC).[29] The JROC was structured to resolve requirements issues among the services, settle debates involving weapons systems development and associated funding, report the validation of requirements to Congress, and ensure joint interoperability. The importance of these functions is evident from the level at which the JROC is chaired – the Vice

Chairman of the Joint Chiefs of Staff. The process itself demands each new system be justified in terms of its operational utility as determined by operations research analysis, cost and operational effectiveness evaluations, and modeling and simulation. The very nature of this process places information systems and infrastructures at a significant disadvantage when competing with kinetic weapon systems because of the difficultly in making statistically based operational comparisons.

Change is rendered all the more difficult when we add in the organizational inertia hinted at by Machiavelli and made real by the contemporary parochial interests of governmental departments, military services, and congressional constituencies. Take for example, the issue of creating and training 5,000 intelligence analysts may come at the expense of a new military hardware program. The advocates for a new military hardware program will clearly state the operational utility of such a program in terms of range, lethality, accuracy, reliability, maintainability, durability, and survivability, cost over the Future Years Defense Plan (FYDP) and the life cycle of the program. They will justify the system by relating its capabilities to the validated requirements, which are highlighted in the Defense Department's Planning Guidance and supports the National Military Strategy and National Security Strategy.

On the other hand, the case can be made effectively for the 5,000 intelligence analysts as an effective informational force element within the PIOSF mode of my proposed IOFSM. This conclusion would be far more intuitive than statistical, and would be easily defeated on these grounds alone. Though a single intelligence analyst could glean a tidbit of significant or critical information with greater value as opposed to the cost of developing a multi-billion dollar system, the hardware is more likely to be funded because of the operative word "could". Being able to quantify costs or benefits in a resource-constrained environment will win every time. Congress employs staffs of people to review statistical evidence based on capabilities and performance not on a piece of intelligence information that could be significant. The latter is too hard to quantify.

We have to overcome these changes by figuring out what is the agreed value of informational data. This is the way we need to proceed if we are to convince Congress to fund our informational forces while continuing the development of our kinetic solutions.

CONCLUSION

As the world continues to evolve, it is incumbent on the United States of America, as the lonely superpower, to promote values such as democratic ideals, religious tolerance, and human dignity. The United States has the instruments and the technology to bring our message

to the world in order to foster stability. Using the National Security Strategy and the proposed approach discussed in the information operations force structure model, the United States can create the conditions to meet effective information operations as an emerging strategic concept of the 21st century.

The armies of a balanced informational force and a kinetic force will give the nation the ability to accomplish tasks that will monitor, measure, weigh, and assess the world 's situation and protect the national interests. Specifically, this paper has highlighted the need for such a balanced force structure that includes informational systems or forces and purely physical destructive systems or forces. A proposed model was offered that took into account our nation's Defense Departments Quadrennial Defense Review report, which highlighted six critical operational goals that are needed to be successful in the transformation of the force. An eventual goal was to transform the force in order to assure information systems could with stand an attack and to conduct effective information operations. We also introduced the key elements the Defense Department employs as a part of its information operations capabilities.

Based on the proposed model, the idea of force structure effectiveness ratings were introduced using some historical examples. This was done to validate the proposed model, and to introduce measures for implementation of such a task. As a part of these measures, informational operational elements were reintroduced that the services already employ. However, we need to articulate our arguments for a balanced informational force and a kinetic force within the framework of a model that ties in historical examples while attempting to quantify what we will accomplish in regard to our transformational goals and national security objectives. My proposed model, if somewhat limited, attempts to do just this.

Word Count: 6,035

ENDNOTES

[1] Joint Chiefs of Staff Publication 3-13, *Joint Doctrine for Information Operations,* 9 October 1998, vii.

[2] Department of Defense, *The Quadrennial Defense Review Report,* 30 September 2001, 31.

[3] Department of Defense, *Briefing – Information Operations "OSD Perspective",* OASD (C3I) IO Strategy and Integration Directorate, 21-25.

[4] Joint Chiefs of Staff Publication 3-13, *Joint Doctrine for Information Operations,* 9 October 1998, ix.

[5] Headquarters, Department of the Army, *FM 100-6 Information Operations,* August 1996, 1-9.

[6] Ibid.

[7] Headquarters, Department of the Army, *FM 100-6 Information Operations,* August 1996, 2-4.

[8] Headquarters, Department of the Army, *FM 100-6 Information Operations,* August 1996, 3-13.

[9] Headquarters, Department of the Air Force, *Air Force Doctrine Document 2-5 Information Operations,* 5 August 1998, 1.

[10] Headquarters, Department of the Air Force, *Air Force Doctrine Document 2-5 Information Operations,* 5 August 1998, 2.

[11] Ibid.

[12] Ibid.

[13] Headquarters, Department of the Air Force, *Air Force Doctrine Document 2-5 Information Operations,* 5 August 1998, 9.

[14] Barnett, Roger W. *Naval Information Operations – Opportunities and Imperatives, A Bottom-UP approach,* US Naval War College, 1.

[15] Ibid.

[16] Carl Von Clausewitz, *On War,* translated by Colonel F. N. Maude (London: Penguin Books Ltd, 1968) 119.

[17] Niccolo Machiavelli, *The Prince,* translated by Robert M. Adams (New York: W.W. Norton & Co, 1992), 116.

[18] Dave Trottier, Lt Col USAF, *The Emerging 21st Century Force Structure Paradigm,* National Defense University, 19.

[19] Carl Von Clausewitz, *On War,* edited and translated by Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 80.

[20] Carl Von Clausewitz, *On War,* edited and translated by Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 83.

[21] Joint Chiefs of Staff Publication 3-13, *Joint Doctrine for Information Operations,* 9 October 1998, II-13 and II-14.

[22] Joint Chiefs of Staff Publication, *Joint Vision 2020,* 8.

[23] Dave Trottier, Lt Col USAF, *The Emerging 21st Century Force Structure Paradigm,* National Defense University, 27.

[24] Dave Trottier, Lt Col USAF, *The Emerging 21st Century Force Structure Paradigm,* National Defense University, 33.

[25] Dave Trottier, Lt Col USAF, *The Emerging 21st Century Force Structure Paradigm,* National Defense University, 37.

[26] US Government Accounting Office, *NSIAD-97-134 Operation Desert Storm Air Campaign,* 1997, 69.

[27] Edward C. Mann, COL USAF, *Thunder and Lightning – Desert Storm and the Airpower Debates,* Air University Press, Maxwell Air Force Base, Alabama, 1995, 145.

[28] Dave Trottier, Lt Col USAF, *The Emerging 21st Century Force Structure Paradigm,* National Defense University, 42.

[29] U.S. Army War College, *How the Army Runs, A Senior Leader Reference Book,* Government Printing Office, Carlisle Barracks, PA, 2002, 4-8.

BIBLIOGRAPHY

Campen, Alan. *The First Information War.* Fairfax: AFCEA International Press, 1992.

Dearth, Douglas. *Cyberwar: Security, Strategy, and Conflict in the Information Warfare.* Fairfax: AFCEA International Press, 1996.

Ivany, Robert MG USA. *How the Army Runs: A Senior Leader Reference Handbook.* Carlisle Barracks: US Army War College, 2002.

Joint Staff. *Joint Publication 3-13, Joint Doctrine for Information Operations.* Washington, October 1998.

_____. *Information Operations, A Strategy for Peace, The Decisive Edge in War.* Washington, March 1999.

_____. *Joint Vision 2020, America's Military: Preparing for Tomorrow.* Washington, June 2000.

_____. *Enabling the Joint Vision.* Washington, January 2000.

_____. *Information Operation, Joint Pub 3-13 Overview Briefing.* Washington, June, 2001.

Machiavelli, Niccolo. *The Prince and The Discourses.* New York: The Modern Library, 1950.

Mann III, Edward COL USAF. *Thunder and Lightning: Desert Storm and Airpower Debates.* Maxwell AFB: Air University Press, 1995.

Office of the President of the United States. *The National Security Strategy of the United States of America.* Washington: The White House, September 2002.

Paret, Peter. *Makers of Modern Strategy.* In Collaboration with Gordon Craig and Felix Gilbert. Princeton: Princeton University Press, 1986.

Trottier, Dave Lt Col USAF. *The Emerging 21st Century Force Structure Paradigm.* National Defense University, 2000.

U.S. Department of Defense. *Quadrennial Defense Review Report.* Washington, September 2001.

_____. *Information Operations "OSD Perspective" Briefing.* Washington, June 2001.

_____. *Information Operations, Field Manual 100-6.* Washington: U.S. Department of the Army, 1996.

U.S. Land Information Warfare Activity. *Guide to Operational Support Services.* Washington: U.S. Department of the Army, May 2000.

U.S. Department of the Army. *Information Operations Primer.* Carlisle Barracks: U.S. Army War College, January 2001.

U.S. Department of the Air Force, *Information Operations, Air Force Doctrine Document 2-5.* Washington: U.S. Department of the Air Force, August 1998.

_____. *Information Operations, A Doctrinal Perspective Briefing.* Washington: U.S. Department of the Air Force, October 2001.

_____. *Building Castles on Sand? Ignoring the Riptide of Information Operations.* Maxwell Papers: U.S. Air War College, August 1998.

U.S. Department of the Navy. *Information Operations in the U.S. Navy Briefing.* U.S. Department of the Navy, July 2001.

_____. *Information Warfare in the U.S. Navy Briefing.* U.S. Department of the Navy, July 2002.

_____. *Naval Information Operations – Opportunities and Imperatives, A Bottom – UP Approach.* Newport: U.S. Naval War College, April 1999.

Von Clausewitz, Car. *On War* Edited and Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1989.